大数据时代个人信息数据安全的新威胁及其保护

张茂月
（厦门大学，福建　厦门　361000）

摘　要： 在大数据时代，个人信息数据面临不断增加的知情权、安宁权、处分权和信息泄露的风险，单纯的“隐私权”本身尚不足以有效应对各类新状况，必须加快构建“综合治理模式”。除了制定专门的个人信息保护规范性法律文件外，还需要确立“告知—同意原则”作为信息收集和利用活动的基本原则，并强化技术化手段及打击信息犯罪活动，以应对大数据时代个人信息安全面临的威胁。

关键词： 大数据；个人信息数据；隐私权；告知同意原则
中图分类号： D913　**文献标识码：** A

DOI:10.13580/j.cnki.fstc.2015.07.021

The New Risks of Personal Data Security in the Era of Big Data and Its Protection

Zhang Maoyue
（Xiamen University，Xiamen 361000，China）

Abstract: In the age of big data，personal data is facing the growing risks of infringement of the right to know，the right without disturbing，the right of disposition and risks of leakage of information，but “privacy” is insufficient to regulate all the risks we are facing today. So an “comprehensive management project” is needed，besides the formulation of specific personal information protection act，we should confirm “Note and Consent” as the basic principle of personal information protection，and also through means of technology and cracking down on crimes to cope with the threat personal data violation in the big data era.

Key words: Big data；Personal data；Privacy；Note and consent

1　大数据的特性及其引发的个体信息数据保护危机

大数据在本质上还是电子数据的一种，但是也有其自身独特的特性。第一，数量巨大。早在2012 年全球每天产生的数据就已经达到 2.5EB，这个数字还以大约每 4 个月翻一番的速度迅速增长[1]。第二，快速化。信息产生的速度常常比数量更加重要，MIT 通过手机定位数据对“黑色星期五”当天将车停在梅西停车场的消费者的数量进行推测，可以大致推断出这一商家在当天的营业

收稿日期：2014－10－08
作者简介：张茂月（1988－），男，浙江丽水人，厦门大学法学院博士生；研究方向：法学理论、电子商务法学。

额。第三，多样性。大数据的形态多样，包括了结构化、半结构化和非结构化数据。此外，现代互联网应用呈现出非结构化数据大幅增长的特点，来源形式多种多样，包括各种信息、应用更新、社交网络的图片、传感器读取的信息、手机的定位等，而且不少信息来源的重要方式都是新近才出现的。

但是，伴随大数据而来的还有个人信息数据安全风险的上升。与用户相关的数据信息正在被逐步集中于少数几个机构，这些机构能够通过几乎所有广受欢迎的网站追踪用户的“网络足迹”，而几乎所有的防护技术都在突出问题的严重性和寻求替代性解决方法方面存在重大缺陷[2]。这些缺陷可能对公民个人信息数据造成强烈威胁，甚至那些看似无用琐碎的信息通过不同方式的加工成为有用的信息。在数据安全的视角下，这一过程表现为大数据使得那些看似“安全”的数据碎片按照某种方式处理后，将重新拼接出完整的个人信息数据清单，甚至直接锁定特定个体，从而对个人信息数据安全造成威胁。

2 个人信息数据保护的传统路径及其存在的问题

2.1 大数据时代个人信息安全面临的新状况

大数据所引发的个人信息安全危机已经引发学界的关注，但是对于如何应对，学界有不同的意见。最为流行的观点主张，继续通过扩张民法中“隐私权”的外延来保护个人数据，认为根据不同的保护对象和内容，对大数据的隐私保护还可以进一步细分为位置隐私保护、标识符匿名保护、连接关系匿名保护等[3]。大数据时代社会所面临的局面远比隐私权提出的 19 世纪末期要复杂得多，整个社会关系的网络化链接已经无处不在，社会的联网甚至已经开启由互联网向物联网迈进的进程，我们的信息安全受到不同于以往的安全威胁。

在以电话为代表的模拟数据时代，个人信息的暴露面是有限的，个人信息的传递方式也是单向和小范围的，能够大规模收集、储存、调取公民个人数据的机构也为数不多，主要是政府部门或者少数垄断性的运营单位。在这样的信息存续的形态下，“隐私权”制度足以提供个体所需的信息安全保护力度。

在大数据时代，先前基于信息垄断获取和保存机制形成的数据安全保障模式也逐渐失效。现代社会获取信息变得异常便捷，只要个体接触网络，就必然将其个人信息数据以各种形式传递给服务提供商和其他网络运营者，信息收集和控制不再局限于有限的组织体，而是向所有有意愿获取和利用个人信息的机构扩散。更复杂的是，经过多重交易和多个第三方渠道的介入，个人数据的权利边界消失了，无法追踪个人信息转移的轨迹，也无法查明个人信息被侵犯的责任主体[4]。

2.2 隐私权与个人信息数据保护

首先，从权利属性看，隐私权主要是一种精神性的人格权，并不过分强调其财产价值属性，其救济方式也是以精神损害赔偿为主。而个人信息权集人格利益与财产利益于一体，既包括了精神价值，也包括了财产价值，而且主要是财产价值属性[5]。大数据时代各网络组织对个人信息数据的分析和利用也主要以获取经济效益为目标，而且大数据的特色在于，通过将闲散化的信息数据加工整合之后形成新的数据价值的方式使用个人信息，那些原本呈现“散状分布”的碎片化信息本身很少涉及个人隐私，或者这些信息是在本人知晓并且允许的情况下提供，就不构成“侵犯隐私”，所以难以通过隐私权的方式全面保护个人信息数据。

其次，大数据时代对个人信息数据的利用方式展现出新的趋向，超出了传统隐私权的保护范围。比如基于大数据对人们的行为进行预测，并依据有关结果采取相应行动，这些活动难以为隐私权所涵盖。在美国有家名为“x + 1”的公司，利用追踪技术来收集用户的网站浏览记录并形成数据库。虽然它不记录人们的姓名，但会通过个人的其他各项数据进行交叉比对和汇集，然后通过统计分析，推测上网者的个人喜好[6]。再如某在线音乐网站进行数据挖掘，通过个体听歌风格的变化，来推断其消费行为的变化。常听流行乐的男性突然开始听新潮女生喜欢听的流行歌，那就有较大概率表明此人在谈恋爱。这个时候给他推荐美食、玫瑰和巧克力的广告，效果好得惊人[7]。

最后，从保护措施来看，隐私的保护注重事后救济，且主要采用精神损害赔偿的民法保护方式加以救济。个人信息的保护则以预防为主，且通过法律衡平信息主体和信息控制者之间的利益[5]。在大数据时代即使确知个人数据的隐私风险，也常常无法简单通过传统的隐私权保护手段解决。在现代网络社会，微博、微信、facebook 等互联网服务商既生产数据，又存储、管理和使用数据，其服务的内容和性质决定了它们必然会接触到用户信息数据，无法简单通过技术或立法手段限制其接近和获得用户信息。

所以我们有理由相信，大数据时代个人信息数据难以通过单一的隐私权保护制度进行规制，有必要采取新措施予以应对。实际上问题不在于大数据是否增加了隐私被侵犯的危险，因为这已经是事实，而在于它是否已经改变了风险的性质。如果只是简单地增加了风险，现有的保护隐私的法律规范还能够在大数据时代继续发挥作用，但是如果问题已经发生了质的改变，则我们必须寻求新的解决办法[6]。

3 大数据时代个人信息数据风险的新样态

大数据时代个人信息数据侵权行为作为“网络侵权”的最新样态，已经不止于“简单地增加了风险”，而是已经逐步开始“改变了风险的性质”。

3.1 信息使用的知情权风险——在用户不知情的状况下收集和利用信息

收集信息只是第一步，收集的目的是为了分析和利用信息创造价值。传统商业模式下，一些商业主体也通过各种方式收集和利用客户的信息资料作为商业决策的参考，但是这往往需要掌握第一手资料，并且这其中大部分是在客户知情的情况下提供的有限信息。比如商场通过吸收会员获得消费者的有限范围个人数据，并判断其购物需要，向其发送促销信息。然而在大数据时代，在电子信息技术的支持下，网络技术公司已经无需获得“第一手”的新资料，而是能够通过已经获取的碎片化的数据信息“反向定位”出消费者的个人情况。在这一过程中消费者获得足够的知情权，甚至部分信息的提供和披露是在其本人的授权和知情的情况下进行的，但是对数据进行进一步的加工和拼接、形成新的数据，则是他们所无法预见的。然而，这一“再造”利用在大数据时代却广泛存在，个人信息使用的知情权未获得足够重视。

3.2 信息的“安宁权”风险——在未经同意的情况下推送信息和服务

在网络购物时，当我们通过某种平台完成某项交易后，下次打开各类网页时都会显示和本次搜索相关的广告，而且这些广告还会随着个人搜索兴趣的转变而转变。可见当消费者表露过某项需求信息并被识别后，互联网公司就可以通过技术手段分辨出消费者的需求信息并向其精确推送广告，即使消费者本人并未授权类似推送行为，消费者无法保障自身在网络世界的信息安宁权益。对于具备高科技信息技术的互联网公司来说，这在技术上并不困难。对业内看来是一种广告的精准投放，但对消费者来说这是“被享受”的“服务”，这种推送活动在大数据的支持下更加隐蔽和精准，能够实现“定制化服务”。

3.3 信息的“处分权”风险——个人数据信息被随意共享和交易

在数据被秘密收集的同时，还有一项更为可怕的活动是数据被秘密地共享甚至交易。在现实中大量个人信息数据被作为商品进行交易，但是对这些行为涉及何种违法行为却不无争议。而且除了一些信息“二道贩子”外，一些“正规的公司”也涉足其中，比如 2009 年爆出的山东移动将用户信息出售给“代理商”，并让有发送垃圾短信需求的客户通过该公司发送垃圾短信，严重损害了消费者对个人信息的支配和处分的权利[9]。但是现行法律对于这些交易行为未有明确定性，理论界对于信息数据的性质也存在不同认识。比如信息数据是否享有民法意义上的“所有权”？何种数据违法行为能够成立侵权？这些问题都没有一个明确的结论。

相对于赤裸裸的交易行为而言，“共享”信息显然是一种更加公开的活动。数据库维护者之间通过合作彼此共享信息，加大了个人信息数据的“暴露面”，信息所有者在这一过程中未被给予表达意见和做出决定的权利，他们对于自身信息数据的“处分权”未获重视。2014 年 4 月，阿里巴

巴购入新浪微博公司18%的股份后，双方确认将在用户账户互通、数据交换、在线支付、网络营销等领域进行深入合作。阿里巴巴希望通过用户和大数据的推动，完善整个移动互联网链条[10]。通过这些交易，互联网巨头之间将在用户信息和交易数据方面实现“共享”，但是这种共享本身就是具有交易性质的行为，而且这种共享对于个人信息数据安全的侵害在大数据时代更加值得担忧，因为这些交易活动直接涉及大数据运用后的“成果”的交易，对方所获得的将会是“赤裸裸”的信息数据或者直接信息数据的通道。

3.4 个人信息数据的被动风险——信息数据的泄露危机

互联网上存储的个人信息数据还面临着来自外部侵入的风险，这种侵入常常使得原本隐秘的信息被广泛泄露，这种风险在大数据时代将非常可怕，因为信息一旦泄露损失将难以估计。黑客攻击是最常见的数据泄露风险来源，黑客们通过后门程序、信息炸弹、网络炸弹、D. O. S攻击以及密码破解等方式发动攻击。近些年来，个人信息泄露的事件不断发生，2014年11月27日，媒体爆出130万学生考研信息遭泄露，包括考研者姓名、手机号码、身份证号、家庭住址、学校、报考专业等敏感信息，引发社会忧虑[11]。

更加值得注意的是，在用户信息被泄露后，数据库的运营者常常拒绝将相关情况向用户通报，致使用户无法及时采取措施减少损失，造成信息“二次伤害”。为了应对这一情况，各国纷纷立法加强数据库信息披露义务。在美国，多达40几个州制定法律，要求告知本州居民其个人信息因为数据库安全缺口而被侵害的情况。欧盟的隐私权指令95/46/EC和加拿大的个人信息保护和电子文件法案（PIPEDA）均要求，基于意外泄露和电子攻击造成的数据外泄必须予以披露，不得私下处理[12]。但是中国尚未做出类似规定，也使得消费者面临更加严峻的信息泄露风险。

4 大数据时代个人信息数据危机的应对

面对日益严峻的个人信息侵害风险，建立或升级一个已经存在的数据管理框架，是解决大数据运行问题的重要手段[13]。针对大数据时代下个人信息数据安全的新形势，如何构建一个全方位的综合治理模式值得思考。综合治理模式要求构建一个包含数据形成、储存、加工、使用和销毁的全过程的监控网络，而完善个人信息保护法规，加强对违法犯罪行为的打击，确立合理的指导原则，以及运用技术化手段应对危机是其中重要组成部分。

4.1 制定和完善个人信息保护法规

在个人信息安全日益受到威胁的当下，强化立法保护是应对这一威胁的有效手段。德国出台统一的立法保护个人数据资料，于1977年制定了统一的“联邦资料保护法”。美国虽然没有类似的统一立法文件，但是也通过众多分散的立法文件确立了以隐私权为基础的个人资料保护法律制度，确立了资料隐私权和自决隐私权[14]。美国1974年隐私权法案要求政府部门向个人公布与其相关的信息记录内容，并限制政府部门与他人或其他部门共享个体信息数据的行为。法案同时要求，政府在收集和处理个人数据信息时遵循“公平信息处理条例”[12]。

完善的法律制度是法律保护的前提，中国目前还没有专门的个人信息数据保护法律文件。《个人信息保护法》作为保护个人信息权的专门法律，2005年就已经完成专家建议稿，但是至今尚未出台。在现阶段有关个人资料的保护规范，主要有全国人大常委会于2012年12月通过的《关于加强网络信息保护的决定》，该规定明确国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。此外还散见于一些法规规章之中，例如《中华人民共和国电信条例》第66条，原则性地规定了电信用户依法使用电信的自由和通信秘密受法律保护，除法律规定外，任何组织或者个人不得以任何理由对电信内容进行检查。《计算机信息网络国际联网管理暂行规定实施办法》、《计算机信息网络国际联网安全保护管理办法》等也仅仅原则性地规定，有关互联网服务提供单位需要“为用户提供良好、安全的服务”，而用户“不得擅自进入未经许可的计算机系统，篡改他人信息；不得在网络上散发恶意信息，冒用他人名义发出信息，侵犯他人隐私；不得制造、传播计算机病毒及从事其他侵犯网络和他人合法权益的活动”。这些原则性规定能够对一些涉及网络的“违法行为”

进行规则，但是却无法应对大数据时代一些涉网的“合法行为”对个人信息数据带来的威胁。值得注意的是，2014 年 10 月 10 日起施行的《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（下称《规定》）第 12 条规定，“网络用户或者网络服务提供者”公开“个人隐私和其他个人信息”的需要承担侵权责任。同时，《规定》也确认了以违反社会公共利益、社会公德的方式公开“自然人自行在网络上公开的信息或者其他已合法公开的个人信息”和“以合法渠道获取的个人信息”的侵权责任。但这一规定仅规定了将“公开”相关个人隐私和信息数据作为侵权行为进行规制，仍无法满足在大数据时代个人信息数据的保护需要。

为了应对大数据时代的信息安全挑战，必须加快推动《个人信息保护法》的出台。通过借鉴德国式的统一立法，提升数据立法保护，确立网络服务提供者在信息数据泄露时的及时告知和信息披露的义务，增加个人信息侵权的预防和救济措施，全方位保障个人信息安全。

4.2 确立“告知—同意原则”作为个人信息数据收集和使用的基本原则

“告知—同意原则”是国外信息安全立法和实践领域通行的重要原则，是互联网用户知情权和选择权的重要保障。现实中各类主体均通过各种途径收集个人信息，但是却很少主动公开或者谋求社会公众同意。美国《华盛顿邮报》于 2014 年 11 月 20 日发文称，谷歌公司在人们使用其搜索引擎时，会偷窥其个人电子邮件、观看网络视频等信息。文章举例称一名妇女使用谷歌搜索引擎一段时间之后，她的确切年龄、所用主要语言、涉及个人生活的电子邮件、个人喜好乃至所购置的电脑型号都会被谷歌掌握。但是谷歌并未公布这些信息收集行为，外界只能猜测其掌握用户“提交的所有数据”[13]。

一些西方国家已经确认，“告知—同意原则”为个人信息数据保护的重要原则。美国在其 1997 年颁布的《全球电子商务政策框架》（下称《框架》）中就规定了“告知—同意原则”，该《框架》要求数据收集者应当告知消费者其收集的信息类型和使用方式，并提供限制使用和再利用个人信息的有效手段。“告知—同意原则”通过赋予用户知情权，使其能够更好地判断个人隐私的安全状况后决定是否参与。根据这一原则，消费者在基于非正当使用或披露个人信息而受到伤害时有权要求赔偿[14]。德国宪法法院也于 1983 年通过判决的方式确立了“个人资料自决权”，并将个人对个人信息的权利确认为宪法权利[14]。中国《关于加强网络信息保护的决定》也明确了网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应明示收集、使用信息的目的、方式和范围，并经被收集者同意。此外，还规定信息收集者收集、使用公民个人电子信息，应当公开其收集、使用规则。这些规定在一定程度上确立了“告知—同意原则”的要求。

“告知—同意原则”也有需要进一步明确的方面，比如信息收集者虽然也会提供类似“隐私保护须知”的项目供用户阅读，但是这类条款往往隐藏于选项卡的某个偏远角落，或者被设计成“长篇大论”，导致没人愿意看完整个内容，无法起到“告知”作用，也无法获得用户真实的“同意”。再如，数据在初次收集时无法预见到最具创新性的二次利用时，互联网公司应当如何进行“告知”？在未事先告知的情形下，是否任何针对个人信息数据的分析活动都必须回头去获取每一位用户的许可？这些都是“告知—同意原则”需要回答的问题[8]。过于宽松的标准无法起到保护个人信息数据的作用，但过于严格的告知同意义务将会限制数据潜力的发挥。

4.3 运用技术化手段应对个人信息安全危机

运用技术手段应对科技带来的调整，不仅必要而且有效。在数据安全防护方面，除了使用防火墙和杀毒软件等传统方式外，用大数据技术应对大数据时代的信息安全挑战是一项有益尝试。比如，为了应对骚扰电话和短信，一些互联网科技公司推出了基于大数据库基础上的信息拦截服务软件。这类软件通过建立“来电黑名单”数据库，有效遴选和识别恶意来电和垃圾信息并进行拦截。微软的新版 IE9 浏览器也开始允许用户自行设置并开启广告拦截功能，来阻挡第三方广告。类似的信息技术手段不仅能够有效应对新型数据安全威胁，更重要的是向我们展示了应对信息安全威胁的新思路。

“匿名化”也是保护个人信息的有效手段。所

谓匿名化就是将个人的身份信息从数据库中抹去，这些个人身份信息包括姓名、地址、信用卡号码、出生日期以及社保号码等，剩余的数据才是可以被使用和分享的数据[8]。虽然这一措施也无法完全杜绝个人信息泄露的风险，但是它有助于维护个人信息数据安全，是现阶段可行的防护措施。

4.4 打击个人信息数据相关的违法犯罪活动

中国对于个人信息安全的刑事立法并不十分完善，导致针对个人数据违法犯罪活动十分猖獗。基于大数据时代信息数量的空前巨大和传播速度的空前迅速，加强对这类犯罪活动的打击尤为重要。中国《刑法修正案(七)》第253条规定了针对公民个人信息数据犯罪行为的刑事责任，但是该条规定略显简单，尚有不少需要明确之处。首先，该条规定并未对“公民个人信息”做具体的界定，现实中公民的个人信息内容非常广泛，是否都是刑法的保护范围是有争议的。其次，虽然该条规定的犯罪主体为一般主体，但是当一般主体实施该项犯罪时要受到后半句中“上述规定”表述的限制。与前半段结合来理解，“上述规定”显然应当指的是“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员在履行职责或者提供服务过程中获得的公民个人信息”，其保护范围有限，无法全面保障大数据时代个人信息数据的安全。再者，修正案规定了“情节严重的”才作为犯罪行为予以处罚，但是何为情节严重却没有具体规定，容易引发争议，尚需要明确的界定。

参考文献:

[1] Andrew McAfee, Erik Brynjolfsson. Big Data: the Management Revolution [J]. Harvard Business Review, 2012, (59-69).

[2] Balachander Krishnamurthy, Craig E Wills. Privacy Diffusion on the Web: a Longitudinal Perspective [EB/OL]. [2014-09-05]. http://www2009.eprints.org/55/.

[3] 冯登国，张敏，李昊. 大数据安全与隐私保护 [J]. 计算机学报，2014，(1).

[4] 杨洁. 大数据时代个人信息的司法保护 [N]. 上海法制报，2014-08-27(B05).

[5] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心 [J]. 现代法学，2013，(4)：62-72.

[6] 新华网：美国网民电脑被安装64种追踪技术隐私无处藏 [EB/OL]. [2014-09-24]. http://news.xinhuanet.com/zgjx/2010-09/06/c_13480127.htm.

[7] 瑞星. 大数据时代的个人安全风险 [EB/OL]. [2014-11-26]. http://www.rising.com.cn/newsletter/news/2013-03-19/13371.html.

[8] Viktor Mayer-Schonberger, Kenneth Cukier. Big Data: a Revolution That Will Transform How We Live, Work and Think [M]. New York: John Murray, 2013: 6.

[9] 搜狐网：移动公司出售用户信息十分钟发1.5万垃圾短信 [EB/OL]. [2014-11-28]. http://it.sohu.com/20090315/n262804573.shtml.

[10] 新华网. 阿里巴巴5.86亿美元入股新浪微博 [EB/OL]. [2014-09-11]. http://news.xinhuanet.com/fortune/2013-04/29/c_124648382.htm.

[11] 新浪网. 考研报名信息遭泄露 1万5买130万用户数据 [EB/OL]. [2014-11-28]. http://edu.sina.com.cn/kaoyan/2014-11-28/1258445592.shtml.

[12] June Jamrich Parson, Dan Oja. New Perspectives on Computer Concepts(Fifteenth Edition) [M]. Singapore: Cengage Learning Asia Pte. Ltd, 2013: 536-537.

[13] The White House. Building an Effective Data Governance Framework [EB/OL]. [2014-09-11]. http://searchdatamanagement.techtarget.com/essentialguide/Building-an-effective-data-governance-framework#guideSection1.

[14] 张楚. 电子商务法教程(第2版) [M]. 北京：清华大学出版社，2011：220-223.

[15] 央广网：美媒细述谷歌如何收集用户信息 偷窥用户88%行为 [EB/OL]. [2014-11-29]. http://tech.cnr.cn/techgd/201411/t20141121_516821065.shtml.

[16] The White House. A Framework for Global Electronic Commerce [EB/OL]. [2014-09-13]. http://www.technology.gov/digeconomy/framewk.wpd.

(责任编辑 沈蓉)